Secure Pre-coding and Post-coding for OFDM Systems along with Hardware Implementation

Jehad M. Hamamreh*, Haji M. Furqan*, and Huseyin Arslan*§
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
§Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620
Email: {jmhamamreh, hamadni}@st.medipol.edu.tr, arslan@usf.edu

***Abstract*—An effective and hardware-friendly physical layer security design, composed of a channel-based frequency pre-coder and a post-coder for OFDM-based systems, is proposed. The design is achieved by decomposing the diagonal matrix of the channel frequency amplitude of the legitimate receiver in order to obtain two unitary orthonormal matrices. The first matrix is used as a pre-coder just before the IFFT process at the transmitter, while the second matrix is used as a post-coder just after the FFT process at the receiver. Besides security, the presented design is interestingly found out to work as a shuffler or inter-leaver, which does not only provide secrecy, but also enhances the performance against burst errors. Moreover, a new channel calibration technique is developed to overcome the effect of channel reciprocity mismatch on the proposed scheme. The provided simulations and USRP hardware testbed implementation results validate the effectiveness of the proposed design in achieving practical and reliable secrecy with just minor modifications on the OFDM structure.**

I. INTRODUCTION

Due to the susceptibility of wireless transmission to passive eavesdropping, designing practical physical layer security techniques is of extreme importance in order to provide confidential communication. To cope with this, channel-based security approaches have emerged as a promising solution instead of just relying on the conventional higher layer encryption methods [1], [2]. In the literature, practical signal processing-based security techniques are usually performed by utilizing the degree of freedom that exists in space domain like MIMO, coordinated multi-point (CoMP), relay, etc. However, when there is no spatial degree of freedom, exploiting the time and frequency degrees of freedom of the transmit waveforms becomes of significant importance to safeguard wireless systems against eavesdropping. Moreover, since OFDM is the most commonly used waveform in currently existing systems and it is expected to keep its dominance in future systems like 5G, securing OFDM waveform has drawn the attention of many researchers around the world. It should be mentioned that besides developing techniques tailored to common transmit waveforms like OFDM, there have recently been some efforts to design new inherently secure waveforms as in [3], [4].

In the literature, many OFDM-based security techniques have been proposed. These techniques can be categorized from a high-level viewpoint into four main enabling schemes. First, secret key-based schemes, in which secret random sequences are generated from the channel and then used to either encrypt the data bits on the application layer [5] or encrypt the data symbols on the physical layer such as dynamic coordinate interleaving and constellation rotation schemes [6]. Second, adaptive transmission-based schemes, in which the transmission parameters are adjusted to just meet the QoS requirements of only the legitimate receiver. Among these techniques are pre-equalization and optimal power allocation [7], adaptive modulation with hybrid-automatic-repeat-request (HARQ) [8], and fading-based sub-carriers deactivation schemes [9]. Third, artificial noise (AN)-based schemes [10], in which the AN is designed based on the legitimate receiver's channel so that it only harms Eve's reception, while maintaining an interference free reception at the legitimate user. Fourth, schemes that can exploit OFDM transceiver impairments [11] or conceal some key features in the OFDM signal to provide secrecy [12].

Although the aforementioned security techniques can enhance the OFDM security, many of them (especially the ones with good secrecy performance) are computationally complex and hard to implement in practice. This is due to the fact that they require considerable changes and modifications of the transceiver hardware and/or network protocols. This may result in the need to build new standards that take physical security into account. However, since physical security is not yet practically mature enough, building a new standard, which can ensure compatibility with current and future devices, might be infeasible at the moment. Therefore, designing alternative security schemes, which require little minor modifications and low computational resources, while ensuring good practical secrecy performance, is of significant interest.

In this work, we first propose a simple and hardware-friendly security scheme, in which OFDM sub-channels are shuffled based on the intended user's channel (which is different from unintended user's channel). This is achieved by extracting unitary matrices from the amplitude of the channel frequency diagonal matrix of the legitimate user. These matrices are then used as channel frequency-based pre-coder and post-coder for achieving security in OFDM systems. Interestingly, the presented design is discovered to work as an inter-leaver for the data sub-carriers. Thus, the design not only provides practical secrecy, but also enhances the reliability of the whole system when channel coding is used. Furthermore, a calibration technique is proposed to remove the effect of channel reciprocity mismatch. Moreover, to validate the practicality of the proposed scheme in real life communication scenarios, a real testbed is built and investigated by using USRP hardware devices. This can be considered as a step forward in the direction of moving physical layer security from

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

theory to practice. The provided results prove the efficiency of the design in achieving practical secrecy with just minor modifications on the existing OFDM structure.

The rest of the paper is organized as follows. The system model and its preliminaries are described in Section II. The details of the developed secure OFDM scheme are revealed in Section III. The proposed method for avoiding channel reciprocity mismatch is explained in Section IV. The simulation and experimental hardware-based results are discussed in Section V. Finally, conclusion is drawn in Section VI.

Notations: Vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. $\mathbf{I}$ is the $N \times N$ identity matrix. The transpose, hermitian, and inverse are symbolized by $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$, respectively.

II. Preliminaries and System Model

A single-input single-output (SISO) OFDM system is considered. In specific, the system is composed of a transmitter (Tx), called Alice, aims at communicating confidentially with a legitimate receiver (Rx), called Bob, whereas an eavesdropper, called Eve, is trying to snoop the data communication link between the two legitimate parties (Alice and Bob). The channels experienced by both Bob $\mathbf{h_b} \in \mathbb{C}^{[1\times L]}$ and Eve $\mathbf{h_e} \in \mathbb{C}^{[1\times L]}$ are assumed to be multi-path slowly varying channels with L exponentially decaying taps and Rayleigh fading distribution. In addition, the reciprocity property of the channel is adopted, where the downlink Alice-to-Bob channel $\mathbf{h_b}$ can be estimated from the uplink Bob-to-Alice one $\mathbf{h_a}$, in a time division duplex (TDD) or hybrid systems (TDD with FDD). Moreover, since Eve is a passive node, the realistic assumption, where Alice has no knowledge of Eve's channel, is adopted. Moreover, both Bob and Eve are assumed to experience independent channels as the wireless channel changes according to the locations of the Tx and Rx as well as the environment [4].

At the Tx, the number of frequency complex data symbols to be transmitted is N, which also represents the total number of utilized sub-carriers. Thus, we represent the frequency domain of each OFDM symbol as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & \dots & s_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$. To provide security, the OFDM symbol is precoded by a channel frequency amplitude based-unitary precoder. This precoder is denoted by a unitary matrix $\mathbf{R}$ of size $N \times N$. The design details of this precoder along with its physical meaning will be explained in the next section. The precoded data ($\mathbf{R} \times \mathbf{s}$) is then passed through an IFFT process $\mathbf{F^H} \in \mathbb{C}^{[N\times N]}$, which basically maps the data points to orthogonal sub-carriers. To avert inter-symbol-interference, a cyclic prefix (CP) of length L is inserted by using the CP appending matrix $\mathbf{C} \in \mathbb{R}^{[(N+L)\times N]}$. Thus, the transmitted base-band signal by Alice can be represented as

$$\mathbf{x} = \mathbf{CF^HRs} \in \mathbb{C}^{[(N+L)\times 1]}. \tag{1}$$

After the signal $\mathbf{x}$ passes through the channel and reaches both Bob and Eve, each one of them will first discard the CP part of the signal using $\mathbf{D} \in \mathbb{R}^{[N\times(N+L)]}$ matrix and then perform an FFT process using $\mathbf{F} \in \mathbb{C}^{[N\times N]}$ matrix to

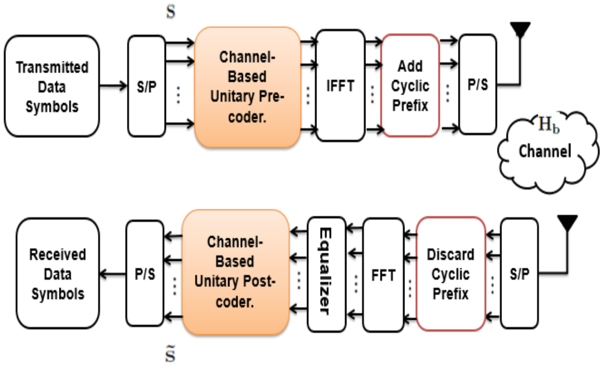


Fig. 1. Structure of the designed secure OFDM scheme.

transform the signal into the frequency domain. Thus, the net received signal vectors at both Bob and Eve after performing the aforementioned operations can be given in a linear matrix representation form, respectively, as follows

$$\begin{aligned} \mathbf{y_b} &= \mathbf{FD}\left(\mathbf{H_bCF^HRs} + \mathbf{z_b}\right) && (2)\\ &= \mathbf{H^f_bRs} + \mathbf{\hat{z}_b}, \in \mathbb{C}^{[N\times 1]}, && (3)\\ \mathbf{y_e} &= \mathbf{FD}\left(\mathbf{H_eCF^HRs} + \mathbf{z_e}\right) && (4)\\ &= \mathbf{H^f_eRs} + \mathbf{\hat{z}_e}, \in \mathbb{C}^{[N\times 1]}, && (5) \end{aligned}$$

where $\mathbf{H_b} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ and $\mathbf{H_e} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ are the Toeplitz matrices of the channel impulse responses of both Bob and Eve, whereas $\mathbf{H^f_b} = \mathbf{FDH_bCF^H} \in \mathbb{C}^{[N\times N]}$ and $\mathbf{H^f_e} = \mathbf{FDH_eCF^H} \in \mathbb{C}^{[N\times N]}$ are the diagonal matrices of the channel frequency responses of Bob and Eve, respectively. The vectors $\mathbf{z_b}$ and $\mathbf{z_e}$ are the zero-mean complex additive white Gaussian noise (AWGN) at Bob and Eve respectively, whilst $\mathbf{\hat{z}_b}$ and $\mathbf{\hat{z}_e}$ are the Fourier transform of the noise at Bob and Eve, respectively.

III. Proposed Secure OFDM Scheme

To secure the communication link between Alice and Bob, the transmitted frequency data symbols are first passed through a pre-coding matrix $\mathbf{R}$, inserted just before the IFFT block, as presented in Fig.1 The pre-coder $\mathbf{R}$ is generated from the channel of the legitimate receiver in such away that the frequency data points or sub-carriers are shuffled at the Tx based on the corresponding amplitudes of their channel frequency response with respect to the legitimate Rx. This is equivalent to making the effective total channel frequency amplitude response (i.e., $\|\mathbf{H^f_bR}\|$) randomly shuffled based on the Bob's channel. The random shuffling process results in a minimum correlation among OFDM sub-channels, making them look completely random at the output of the FFT block. This can be performed by applying a linear matrix decomposition (factorization) process on the amplitude of the diagonal channel matrix of Bob $\|\mathbf{H^f_b}\|$. Without loss of generality, we can obtain the pre-coder $\mathbf{R}$ by employing any of the common linear factorization methods. For simplicity and familiarity,

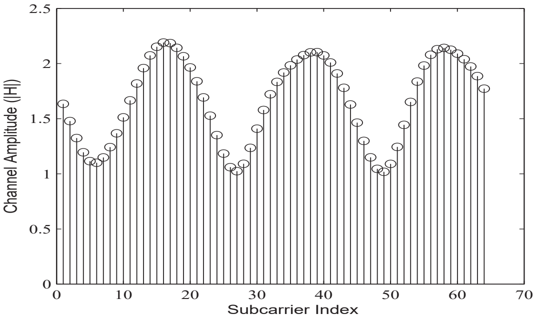


Fig. 2. The channel frequency amplitude $\|\mathbf{H_b^f}\|$.

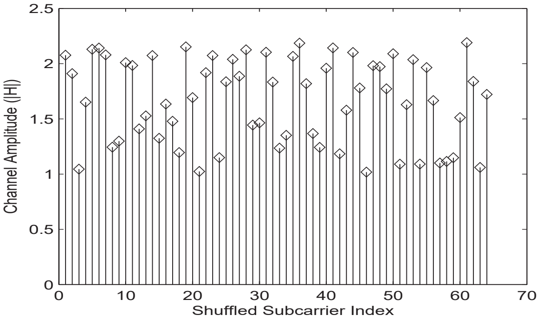


Fig. 3. The channel frequency amplitude of $\|\mathbf{H_b^f}\|\mathbf{R}$ (shuffling).

SVD is chosen as the underlying method. Consequently, $\|\mathbf{H_b^f}\|$ can be represented by the following new decomposed matrices:

$$\|\mathbf{H_b^f}\| \;=\; \underbrace{\mathbf{U}}\underbrace{\mathbf{E}}\underbrace{\mathbf{V}^T}, \tag{6}$$

where $\mathbf{U}$ and $\mathbf{V}$ are unitary orthonormal matrices, whereas $\mathbf{E}$ is a diagonal matrix with real entries. Note that since $\|\mathbf{H_b^f}\|$ is a diagonal matrix with real values $\|\mathbf{H_b^f}\| = diag\{\|H_{1b}^f\|, \|H_{2b}^f\|, \cdots, \|H_{Nb}^f\|\}$, the two unitary matrices ($\mathbf{U}$ and $\mathbf{V}$) are equal and the value of each entry in any of the unitary matrices is either zero or one. Also, in each column of the matrices, there is only one entry whose value equals to one, while the rest are zeros. Accordingly, the precoding matrix $\mathbf{R}$ can be equal to any of the following matrices to perform channel shuffling as given below:

$$\mathbf{R} \;=\; \mathbf{U^T} = \mathbf{V^T} \in \mathbb{R}^{[N\times N]}. \tag{7}$$

Assuming that we have a realistic channel impulse response of $L = 9$ taps with exponential power delay profile and the fading amplitude's distribution of each tap is Rayleigh. Then one possible realization of $\|\mathbf{H_b^f}\|$ can be given as in Fig.2. When $\mathbf{R}$ is used as a precoding matrix, then the effective channel amplitude response ($\mathbf{H_b^f R}$) becomes randomized and shuffled as shown in Fig.3.

Therefore, to perform channel-based shuffling, Alice can use $\mathbf{R}$ as a pre-coding matrix. Since the column vectors of $\mathbf{R} = \begin{bmatrix}\mathbf{r}_1 & \mathbf{r}_2 & ... & \mathbf{r}_N\end{bmatrix}$ are orthogonal to each other with zeros and ones entries, Alice can use them as randomizing vectors to change the order of the transmitted symbol based on the legitimate channel. This results in a block of symbols experiencing uncorrelated, randomized channel states as shown in Fig.3. This process can mathematically be given as

$$\mathbf{d} \;=\; \sum_{i=0}^{N-1} s_i \mathbf{r}_i \in \mathbb{C}^{[N\times 1]}. \tag{8}$$

It should be noted that each one of the complex modulated symbols, s_i, is basically mapped to a new position (index) based on the amplitude of the channel frequency response, where the mapping process is implemented via a simple multiplication operation between each data symbol and an orthonormal vector of length N with all positions zeros except one at the index of the new position. The operation in (8) can further be simplified into a matrix form as

$$\mathbf{d} \;=\; \mathbf{Rs} = \mathbf{V^T s} \in \mathbb{C}^{[N\times 1]}. \tag{9}$$

From a signal processing point of view, this is somehow similar to the concept of interleaving [13], whose goal is to randomize the burst errors in the channel, but here a new and much simpler design is devised to achieve perfect interleaving from a physical layer security perspective. Besides secrecy, this can significantly enhance the performance of the channel codes, which are usually suitable for correcting random errors, but not burst ones. Since frequency channel amplitude states are correlated as shown in Fig. 2, consecutive occurrence of ”Good” or ”Bad” subchannels is anticipated in the trellis decoder if no interleaving is used. This is unfavorable because the Viterbi decoder selects a correct path or an error path based on the cumulative decision metrics controlled by the path. It should be mentioned that investigating the performance of the proposed scheme with channel coding is out of the scope of this paper and left as a future work.

At the Bob's side, the baseband received signal after S/P conversion, CP removal, and FFT processing, can be given as

$$\mathbf{y_b} \;=\; \mathbf{H_b^f d} + \mathbf{\hat{z}_b} = \mathbf{H_b^f R s} + \mathbf{\hat{z}_b}. \tag{10}$$

Bob then performs zero forcing equalization via multiplying $\mathbf{y}$ with the inverse of $\mathbf{H_b^f}$ to get $\hat{\mathbf{y}}$ as given below

$$\begin{aligned} \mathbf{\hat{y}_b} \;&=\; [\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_N]^T = \left(\mathbf{H_b^f}\right)^{-1} \mathbf{y_b} && (11)\\ &=\; \mathbf{d} + \mathbf{\hat{\hat{z}}_b} = \mathbf{Rs} + \mathbf{\hat{\hat{z}}_b}, && (12) \end{aligned}$$

where $\mathbf{\hat{\hat{z}}_b} = \left(\mathbf{H_b^f}\right)^{-1} \mathbf{\hat{z}_b}$. Then, Bob applies SVD on $\|\mathbf{H_b^f}\|$ to get $\mathbf{R^T} = \mathbf{U} = \mathbf{V}$, which works as the inverse of $\mathbf{R}$. Since the column vectors of $\mathbf{R^T} = \begin{bmatrix}\mathbf{r}_0^T & \mathbf{r}_1^T & ... & \mathbf{r}_N^T\end{bmatrix}$ are orthogonal to each others, Bob can use them as inverse basis vectors to return the data symbols to their original positions. This can be implemented as follows:

$$\mathbf{\hat{s}} \;=\; \sum_{i=1}^{N} \hat{y}_i \mathbf{r_i^T} \in \mathbb{C}^{[N\times 1]}. \tag{13}$$

Another representation for this process is to directly multiply $\hat{\mathbf{y}}$ by $\mathbf{R^T}$ as given below

$$\begin{aligned} \mathbf{R^T}\hat{\mathbf{y}}_\mathbf{b} &= \mathbf{R^T}\left(\mathbf{d}+\hat{\mathbf{z}}_\mathbf{b}\right) = \mathbf{R^T}\mathbf{R}\mathbf{s} + \mathbf{R}\hat{\hat{\mathbf{z}}}_\mathbf{b}, \quad (14)\\ \hat{\mathbf{s}} &= \mathbf{s} + \mathbf{R^T}\hat{\hat{\mathbf{z}}}_\mathbf{b}. \quad (15) \end{aligned}$$

On the eavesdropper's side, the captured signal is given by

$$\mathbf{y_e} = \mathbf{H^f_e}\mathbf{d} + \hat{\mathbf{z}}_\mathbf{e} = \mathbf{H^f_e}\mathbf{R}\mathbf{s} + \hat{\mathbf{z}}_\mathbf{e}. \quad (16)$$

Although Eve is assumed to have a complex receiver with full knowledge of the transmission technique, she will not be able to decode the data correctly. This is due to the fact that her channel is different from Bob's one. Therefore, when Eve tries to extract a post-coder that can cancel the effect of the precoder used at the Tx, she will obtain a post-coder totally different from Bob's one, making her unable to decode. In this situation, Eve will be forced to perform an extremely exhaustive search process, trying to find some matrices that might reduce errors. However, this would be impractical as the matrix size is relatively huge and can be increased with the increase of the sub-carriers number. Also, since the variation nature of wireless channels provides repeatedly renewed randomness, the proposed secure OFDM design would be updated frequently, which further increases the robustness of the security design. Thus, from a signal processing perspective, Eve cannot decode the data correctly.

IV. Proposed Method for Avoiding Channel Reciprocity Mismatch

Due to the fact that practical wireless TDD systems suffer from having imperfect channel reciprocity (ICR), detrimental side effects can occur when physical layer security techniques are employed due to their channel reciprocity-dependent nature. For instance, channel-based key generation techniques [14] may result in severe BER performance degradation if the generated keys from the channel are not exactly the same at Alice and Bob. To alleviate this problem, several reconciliation methods were proposed in the literature [14] to correct the mismatch that exists in the generated sequences at Alice and Bob. In this process, the mismatch can be removed by the exchange of an information sequence, which is publicly sent through the channel, and thus Eve can easily know part of the generated key. Therefore, privacy amplification is usually used after reconciliation to reduce the amount of leaked information to Eve, but this will decrease the secret key rate. Another issue is that current reconciliation methods are designed to work for sequences of binary random variables, but not matrices of any random variables (as in the case of our proposed secure design). Thus, due to the problems associated with reconciliation and resulted from reciprocity mismatch, in this section, we develop and propose a new practical calibration technique to overcome both the problem of channel reciprocity mismatch (CRM) and the reconciliation-related issues. The proposed technique is inspired by the calibration technique used in 802.11n WiFi standard [15]. However, in the standard the technique was designed without having security in mind, and thus although it can solve the reciprocity problem, it fails to tackle the security problem as the receiver is forced to send publicly a quantized version of the estimated channel to the transmitter. This makes Eve aware of the legitimate user channel, resulting in a security breach as Eve can extract whatever Alice extracts. In the proposed technique, which is summarized in Fig.4, channel reciprocity problem is solved without compromising secrecy at all.

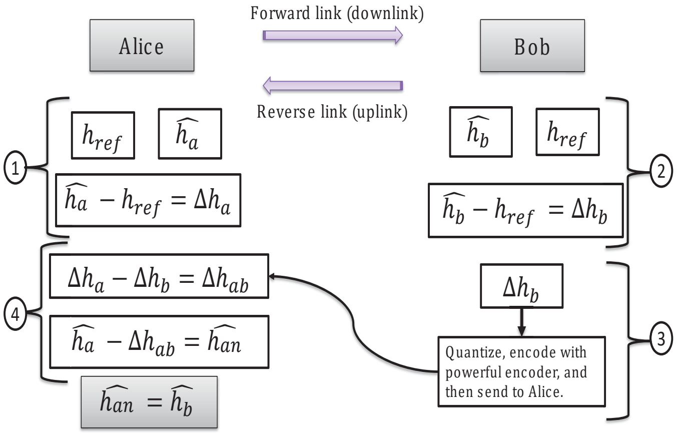

Forward link (downlink)
Alice
Bob
Reverse link (uplink)
h_{ref}
$\widehat{h_a}$
$\widehat{h_a} - h_{ref} = \Delta h_a$
1
$\widehat{h_b}$
h_{ref}
$\widehat{h_b} - h_{ref} = \Delta h_b$
2
$\Delta h_a - \Delta h_b = \Delta h_{ab}$
$\widehat{h_a} - \Delta h_{ab} = \widehat{h_{an}}$
$\widehat{h_{an}} = \widehat{h_b}$
4
Δh_b
Quantize, encode with powerful encoder, and then send to Alice.
3

Fig. 4. Procedure of the proposed method for avoiding channel reciprocity mismatch between Alice and Bob.

Without loss of generality, the basic idea is to let Alice and Bob agree on a reference channel $\mathbf{h_{ref}}$, with which they can compare their channels, and then make use of their differences to compensate the effect of CRM. More precisely, assuming that both Alice and Bob have their estimated erroneous channels (i.e., $\widehat{\mathbf{h_a}}$ and $\widehat{\mathbf{h_b}}$) and a copy of $\mathbf{h_{ref}}$, which can be obtained from a shared random sequence between the legitimate parties [12], then both Alice and Bob can find their channel differences ($\mathbf{\Delta h_a}$ and $\mathbf{\Delta h_b}$) with respect to $\mathbf{h_{ref}}$. Afterwards, Bob quantizes its channel difference $\mathbf{\Delta h_b}$, encodes it using a powerful encoder, and sends it publicly to Alice. Although $\mathbf{\Delta h_b}$ is transmitted publicly, Eve will not be able to get any information about Bob's channel because $\mathbf{\Delta h_b}$ represents the difference between two random unknown sequences. Alice then uses $\mathbf{\Delta h_b}$ to find $\mathbf{\Delta h_{ab}}$ by subtracting $\mathbf{\Delta h_b}$ from $\mathbf{\Delta h_a}$. Finally, Alice subtracts $\mathbf{\Delta h_{ab}}$ from $\widehat{\mathbf{h_a}}$ to get a calibrated channel, denoted as $\widehat{\mathbf{h_{an}}}$, which is exactly equal to Bob's estimated channel $\widehat{\mathbf{h_b}}$. Thus, similar channels at both Alice and Bob are obtained. By utilizing this calibration technique, our proposed security method can be applied reliably without worrying about CRM problem.

V. SECURE OFDM TESTBED SETUP AND RESULTS

This section presents the implementation of the proposed hardware-friendly security design. In specific, an OFDM testbed is developed by using Labview, Matlab, and USRP devices to verify and investigate the proposed security scheme in a realistic scenario. The hardware setup consists of three USRPs, each with a single antenna of type VERT-900.

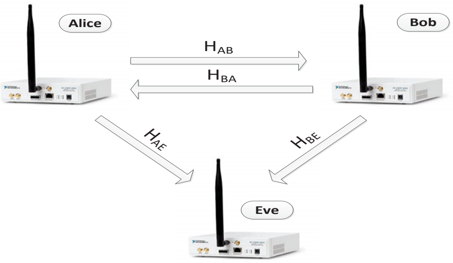


Fig. 5. Basic hardware testbed setup using USRP devices.

TABLE I
SYSTEM PARAMETERS

Frequency	910MHz
Modulation	QPSK
USRP model	USRP 2932
Antenna	VERT-900 Vertical
IQ rate	500K
No. of QAM symbols per frame	625 symbols
No. of pilots symbols	25 symbols
QAM symbols+Pilots per OFDM-symbol	150 symbols
FFT size	256
(Symbol + ZP+ CP) per OFDM-symbol	320 symbols
No. of OFDM symbols per frame	5 symbols
Synchronization method	Van de peek Algorithm

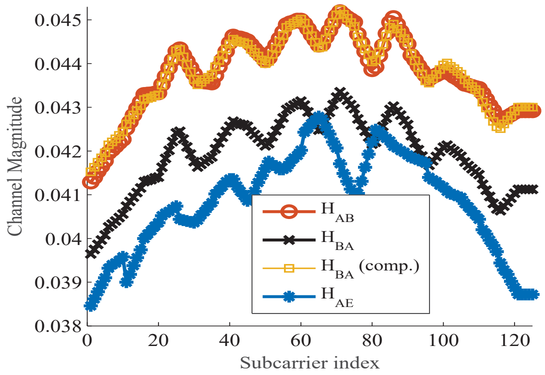


Fig. 6. The real estimated channel Freq. magnitudes at Bob, Alice and Eve.

The basic block diagram of the hardware setup is presented in Fig.5, where H_{AB}, H_{BA}, H_{AE}, H_{BE} are the channel observations between Alice-to-Bob, Bob-to-Alice, Alice-to-Eve, and Bob-to-Eve, respectively. It should be noted that H_{AB}=$\mathbf{H_b}$ and H_{AE}=$\mathbf{H_e}$ with respect to notations used in Section II and III. In the setup, one USRP acts as Alice (legitimate transmitter), other USRP acts as Bob (legitimate receiver), while the third USRP acts as Eve (illegitimate receiver). Alice and Bob were separated by 1.5m and Eve was 1m away from them. For simplicity, all the USRPs have the same configuration in software and hardware and all are connected to a single central computer. The computer applies signal processing on the transmitted and received streams via Labview and Matlab. For channel estimation, pilot symbols are added in each OFDM symbol after every 5th QAM symbol and after that zero padding (ZP) and cyclic prefix (CP) are also added for reducing out of band emission (OOB) and avoiding inter symbol interference (ISI), respectively. The details of the used system parameters are given in Table 1.

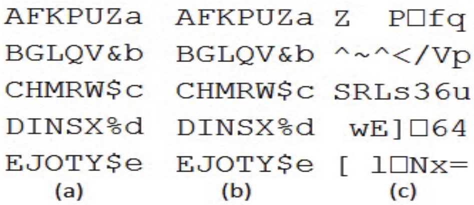
After adjusting the three USRPs and their parameters, we let the devices to start communicating with each others. A string of alphabetical symbols is used for data transmission, which is converted to ASCII code, reshaped, and then stored into a buffer for transmission.

As described in Section III, since the estimation of the channel frequency amplitude is required at Alice and Bob, a channel sounding process must be performed before the communication starts. To do so, Alice sends to Bob a sequence of OFDM pilot symbols for channel estimation, since Bob knows the sequence a head of the time, Bob can just divide it by its own to estimate the channel H_{AB}. On the other side, Bob sends back to Alice another sequence of OFDM pilot symbols, which is also already known to Alice so that the channel H_{BA} can be estimated. Note that Eve is assumed to know the pilot symbols and thus can estimate its channel normally without difficulties.

Fig.6 presents the average of channel estimations at Bob (H_{AB}), Alice (H_{BA}) and Eve (H_{AE}). The estimated channel between Alice to Bob (H_{AB}) and Bob to Alice (H_{BA}) are represented by marker $\circ$ and $\times$, respectively. It is observed from the measurements visualized in Fig.6 that the channel frequency amplitudes of Alice-to-bob (H_{AB}) and Bob-to-Alice (H_{BA}) are approximately reciprocal but there is a small mismatch due to RF front end impairments. The mismatch is removed by employing the calibration technique explained in Section IV. The compensated channel estimate from Bob-to-Alice (H_{BA} (comp)) is presented in Fig.6 by marker $\square$. Fig.6 also presents the estimated channel at Eve (H_{AE}) as shown by marker $*$. It is clear that Eve has different channel observations due to spatial decorrelation of wireless channels [16].

Alice uses compensated H_{BA}, while Bob uses H_{AB} for generating the precoding and postcoding matrices, respectively. Once the channels are obtained at both sides, both Alice and Bob first diagonalize the estimated channel vector and then apply SVD decomposition to get the precoding and postcoding matrices, respectively (as explained in Section III). Alice uses $\mathbf{R}$ for shuffling in order to secure data from Eve, while Bob applies $\mathbf{R^T}$ to get the original version of the transmitted data.

Since the proposed scheme does not change the received signal-to-noise-ratio (SNR) at any of the receivers (i.e., Bob or Eve), secrecy rate or secrecy outage probability metrics are not applicable here as they cannot reflect the practical secrecy obtained by this scheme. Due to this, the performance is evaluated in two alternative ways. First, by sending real data message and show its decoded result. Second, by simulating the BER performance [1], [4]. In the first case, a data message related to the character string ('ABCDEFGHIJKLMNOPQRSTUVWXYZ&$%abcde') is sent by Alice and



```
AFKPUZa  AFKPUZa Z  P□fq
BGLQV&b  BGLQV&b ^~^</Vp
CHMRW$c  CHMRW$c SRLs36u
DINSX%d  DINSX%d  wE]□64
EJOTY$e  EJOTY$e [ 1□Nx=
  (a)      (b)      (c)
```

Fig. 7. (a). Transmitted data from Alice, (b). Received data at Bob, (c). Received data at Eve.

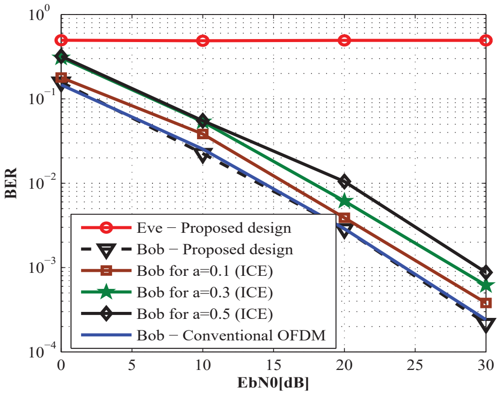


Fig. 8. BER of both Bob and Eve using the proposed secure OFDM design. Modulation is QPSK, N=64 sub-carriers, and L=9 channel taps.

then received by both Bob and Eve. Fig.7 (a) shows the transmitted data from Alice, while Fig.7 (b) and (c) present the decoded messages (received data) at both Bob and Eve, respectively. It is observed that Bob can successfully decode the data, but Eve cannot decode the data correctly.

Fig.8 shows the BER performance of both Bob and Eve using the proposed design. It is shown that the Bob's BER performance using the proposed scheme is the same as the conventional OFDM system in the case of perfect channel estimation. However, a slight BER degradation is observed when imperfect channel estimation (ICE) is considered. Particularly, the effect of ICE is investigated at three different error variances with $a = 0.1$, $a = 0.3$, and $a = 0.5$, where ICE is modeled as an independent complex Gaussian noise with zero mean and error variance $\sigma^{\mathbf{2}}{}_{T/R} = a \times 10^{\frac{-SNR_{dB}}{10}}$. It is clear that as the channel estimation quality enhances (i.e., low error variance), the BER performance gets better. Fig.8 also depicts the severely bad BER performance of Eve although she is assumed to be aware of the method. This occurs due to the use of channel-dependent precoder over Alice-to-Bob channel, which is different from Alice-to-Eve channel. Compared to [6], our design is not only new and simpler, but can also provide full secrecy rate with almost zero error mismatch thanks to the novel channel calibration technique we have developed.

VI. CONCLUSION

A channel frequency-based pre-coder and post-coder design for achieving security in OFDM systems is introduced. The design is achieved by extracting orthonormal matrices obtained from applying SVD on the diagonal matrix of the legitimate user's channel frequency amplitude. The presented design is shown to work as a shuffler for the data sub-carriers, leading to avoid burst-errors. This can consequently enhance the reliability performance of the OFDM system when channel coding is used. Moreover, the practicality of the proposed scheme has been validated by building a real testbed using USRP hardware devices. The presented results have proven that the proposed design achieves practical secrecy without increasing the complexity of the OFDM structure.

ACKNOWLEDGMENT

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

REFERENCES

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surv. Tuts*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, "A Practical Physical-Layer Security Method for Precoded OSTBC-Based Systems," in *2016 IEEE Wireless Communications and Networking Conf. (WCNC)*, April 2016, pp. 1651–1656.

[3] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform Design for Secure SISO Transmissions and Multicasting," *IEEE J. Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[4] J. M. Hamamreh and H. Arslan, "Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2017.

[5] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *J. Commun. Networks*, vol. 14, no. 4, pp. 385–395, Aug. 2012.

[6] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[7] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-Efficient Resource Allocation for Secure OFDMA Systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[8] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY Layer Security Design Using ARQ with MRC and Adaptive Modulation," in *2016 IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1632–1638.

[9] E. Guvenkaya and H. Arslan, "Secure Communication in Frequency Selective Channels with Fade-avoiding Subchannel Usage," in *2014 IEEE Int. Conf. Commun. Work. ICC 2014*, Jun. 2014, pp. 813–818.

[10] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[11] M. Yusuf and H. Arslan, "Controlled Inter-carrier Interference for Physical Layer Security in OFDM Systems," in *IEEE Vehicular Technology Conference (VTC-Fall)*, Sept 2016, pp. 1–5.

[12] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," in *2014 IEEE Military Communications Conference*, Oct 2014, pp. 485–489.

[13] S.-W. Lei and V. K. N. Lau, "Performance Analysis of Adaptive Interleaving for OFDM Systems," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 3, pp. 435–444, May 2002.

[14] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on Channel Reciprocity Based Key Establishment Techniques for Wireless Systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[15] I. S. 802.11n, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Throughput*, IEEE Std., Sep. 2007.

[16] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, Sept 2016, pp. 597–602.